A Unique Identity bill*

Usha Ramanathan

India's unique identification number project has been sold on the promise that it will make every citizen, the poor in particular, visible to the State. But the UID project raises crucial issues relating to profiling, tracking and surveillance, and it may well facilitate a dramatic change in the relationship between the State and the people. The Unique Identification Authority of India has not acknowledged these concerns so far. And now, nowhere in the proposed draft bill that it has prepared have these issues been addressed nor have clauses been drafted to prevent abuse of information that will be collected by the agency. With so many questions on the project — regarding biometrics, security and privacy — yet to be answered, it is far from time for parliamentary approval. As has been observed, the Constitution is expected to provide the citizen with dignity and privacy; but these are missing in the UID project.

In February 2009, the unique identification number (UID) project was set up within the Planning Commission. Since August (July) 2009, when Nandan Nilekani was appointed as its chairperson, the Unique Identification Authority of India (UIDAI) has been propagating the idea of the UID which each resident in India will be given.

The project pegs its legitimacy on what it will do for the poor. It promises that it will give the poor an identity, with which they may become visible to the state. The UID number is expected to plug leakages, including in the Public Distribution System (PDS), ease payments to be made under the National Rural Employment Guarantee Scheme (NREGS), and enable achievement of targets in consonance with the right to education. Service delivery is a central theme in its promotional literature. The raising of expectations is, however, tempered by a quick caveat that the "UID number will only guarantee identity, not rights, benefits, or entitlements".

The UID database is intended to hold information including the name, address and biometrics of the person. It has been reiterated with remarkable regularity that

*Thanks to Pavithra Ramesh and Murali for acting as sounding boards.

the UIDAI will not be gathering information that could lead to profiling, so, religion, caste, language and income, for instance, will not be brought on to the UID database.

The UIDAI has strained every nerve to explain that it will not be a database from which others may derive information about any person. The UIDAI will merely "authenticate", i.e., it will give a "yes" or "no" answer when asked whether a name, address and biometric indicator tally. That is, it will attest to the veracity of the identity being asserted by a person by checking on its database. If the details tally, it will say no more.

The operation for being invested with an identity goes through stages: enrolling with an enroller/registrar who will set down the basic biographic details such as name, address, father/guardian's name (and UID number), mother's name (and UID number) and collect the biometrics — photographs, all 10 fingerprints and iris scan, de-duplication (which will be done by the UIDAI to make certain that there is one identity for one person), updating the database whenever any change occurs in relation to the information on the database (for instance, when there is a name or address change, the responsibility for which will rest with the individual).

The UIDAI has said that getting on to the UID database is voluntary. That is, it is clarified, there will be no compulsion from the UIDAI. But, if other agencies make the UID number essential in their transactions, that is a different matter. The UIDAI has been signing memoranda of understanding (MOUs) with a range of agencies including banks, state governments and the Life Insurance Corporation of India (LIC) to be "registrars", who then may insist that their customers enrol on the UID to receive continued service.

Given the dramatic changes that the UID could bring to the relationship between the state and the people, it should cause concern that there has been so little public debate around the UID. There is an unquestioned benignness that is being attributed to the project, which could be explained in part by the image of Nandan Nilekani, whose salience to the project could foster a sense that this is a project around technology, and not about identity. The rhetoric has stayed focused on the poor, which has lent the project legitimacy and there has been no discussion from within the establishment on the possible downsides.

One concern that has been raised consistently is on the question of privacy — that information held in a central repository could result in breaches of privacy. The invasion of privacy that technology has facilitated and routinised in recent years has eroded the relevance of traditional notions of privacy. The experience with abandoning the idea of privacy is relatively recent, and it will be a while before its value is reconstituted and the idea resurrected. The introduction to the UID has been in terms of investing every resident with an identity, as a single stop for

authenticating identity, as a de-duplication exercise, for plugging leakages, as a tracking device, and as a wage transferring device.

There are, however, other concerns that have been voiced and which remain unresolved. They include the contexts of convergence, national security, the national population register (NPR), and the shaky edifice of biometrics on which this superstructure is being built.

Convergence

The UID literature does not use the word, yet convergence is a predictable and inevitable consequence of the UID project. Convergence is about combining information. There are various pieces of information that we hand over to a range of agencies when buying, say, a railway ticket, maintaining a bank account, registering in a university, getting work at an NREGS worksite, taking out an insurance policy, buying a motorcycle, paying telephone bills, etc. Currently, with only the name and a possibly correct address, it will not be easy to profile a person or track them. The information is held in what are called "silos", that is, discrete towers holding information that has been handed over by an individual in relation to a defined purpose. If it were possible to create bridges to link these silos, it would wrest control of information on the individual and make it available, metaphorically and literally, at the tap of a computer key.

There is a dark joke making its rounds which would be funny, but is not, and it runs like this:

> Operator: Thank you for calling Pizza Plaza. May I have your ...
>
> Customer: May I place an order?
>
> Operator: Can I have your multipurpose *ID* card number, sir?
>
> Customer: It is, hold on ... 21356102049998–45–54610
>
> Operator: Welcome back from Japan, Mr Singh.
>
> Customer: May I order your Seafood Pizza ...
>
> Operator: That's not a good idea, sir.
>
> Customer: Why would you say that?
>
> Operator: According to your medical records, sir, you have high blood pressure and even higher cholesterol level.
>
> Customer: What? ... What do you recommend then?

Operator: Try our Low Fat Pizza. You'll like it.

Customer: How would you know that?

Operator: You borrowed a book titled *Popular Dishes* from the National Library last week, sir.

Customer: Oh ... Have three family size delivered. How much would that cost? Operator: That should be enough for your family of 5, sir. That will be ₹500.

Customer: Do you accept payment by credit card?

Operator: I'm afraid you have to pay us cash, sir. Your credit card is over the limit and you owe your bank ₹23,000 since October last year. And that's not including the late payment charges on your housing loan.

Customer: I guess I have to run to the neighbourhood ATM and withdraw some cash before your guy arrives.

Operator: Oh, no, sir. Your records show that you've reached your daily limit on machine withdrawal today.

Customer: Never mind, just send the pizzas, I'll have the cash ready. How long will that take?

Operator: About 45 minutes, sir, but if you can't wait you can always come and collect it in your Nano. Will there be anything else, sir?

Customer: No ... By the way ... make sure you send the 3 free bottles of cola as advertised.

Operator: But, sir, your health records say you're a diabetic. ...

Customer: #$$^%&$@$% ^

Operator: Please watch your language, sir. Remember on 15 July you were convicted of using abusive language at a policeman ... ?

It was reported last year that Apollo Hospitals had written to the UIDAI and to the Knowledge Commission to link UID numbers with health profiles of individuals and offered to manage the health records (*Business Standard*, 27 August 2009). It has already embarked on a project "Health Superhighway" that reportedly connects doctors, hospitals and pharmacies, who would be able to communicate with each other and access health records. This, then, is no longer hypothetical. The UID is poised to be the bridge between silos of personal information.

This convergence of information may be efficient for business and meet standards of efficiency, but there are those who would argue that it profiles individuals and exposes them to market and other forces in ways which are intrusive, and which could make them insecure, and unsafe.

National Security

Surveillance is a concern, and a term that is missing altogether in the UIDAI documents.

There are three initiatives that, together, form a pattern that is disturbing. The UID only produces a number which is a tag that is poised to be "universal" and "ubiquitous". Its capacity to link disparate pieces of information is difficult to dispute. Place this in the context of the National Intelligence Grid (NATGRID), and the Home Minister P Chidambaram's statement begins to sound ominous. "Under NATGRID", he is reported as having said, "21 sets of databases will be networked to achieve quick seamless and secure access to desired information for intelligence and enforcement agencies" (*The Hindu*, 14 February 2010). This is to enable them "to detect patterns, trace sources for monies and support, track travellers, and identify those who must be watched, investigated, disabled and neutralised". Many of these intelligence agencies, including the Research and Analysis Wing (RAW) and the Intelligence Bureau (IB), are neither creatures of the law, nor are they subject to oversight. And they are outside the Right to Information Act. Vice-President Hamid Ansari, quoting an intelligence expert, reportedly asked: "How shall a democracy ensure its secret intelligence apparatus becomes neither a vehicle for conspiracy nor a suppressor of traditional liberties of democratic self-government?" (*Times of India*, 20 January 2010). By all accounts, the question has not been answered yet.

In November 2009, newspapers reported Chidambaram's statement that the government would soon be setting up a DNA data bank. There has been no word on the subject since, but on 12 July 2010, the *Indian Express* carried news of an impatient debate that has erupted about speeding up DNA data banks to hold DNA data of convicts. This is just a stretch away from extending it to more classes of the population.

The use of science and technology to practise the politics of suspicion is a possibility that is finding its way into becoming a fact.

National Population Register

The Census has acquired a disturbing dimension with the NPR being appended to it. The NPR is not an exercise undertaken under the Census Act, 1948. It is being carried out under the Citizenship Act of 1955 and the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules 2003. Why should that matter? Because there is an express provision regarding "confidentiality" in the Census Act, which is

not merely missing in the Citizenship Act and Rules. But there is an express objective of making the information available to the UIDAI, which marks an important distinction between the two processes. Section 15 of the Census Act categorically makes the information that we give to the census agency "not open to inspection nor admissible in evidence". The Census Act enables the collection of information so the state has a profile of the population; it is expressly not to profile the individual.

It is the admitted position that the information gathered in the house-to-house survey, and the biometrics collected during the exercise, will feed into the UID database. The UID document says the information that the database will hold will only serve to identify if the person is who the person says he, or she, is. It will not hold any personal details about anybody. What the document does not say is that it will provide the bridge between the "silos" of data that are already in existence, and which the NPR will also bring into being. So, with the UID as the key, the profile of any person resident in India can be built up.

The Citizenship Rules 2003 strips the veneer of voluntariness from the UID. It classes every individual and every "head of family" as an informant, who will be penalised if every person in the household is not in the NPR, or if the information is outdated.

The NPR is also slated to collect biometrics — photographs, fingerprints, iris. The coercion in the Citizenship Rules is not the only aspect which is worrying. The rules also envisage an exercise in sifting the citizen from the resident. The person collecting the information is expected to exercise judgment in deciding whether the person whose details are being taken down may not be a citizen. If there is any doubt, such person will be categorised to be subject to further investigation. The NPR, like the Census, is carried out by laypeople, and the untrained mind is asked to discern and judge matters that could lead to inclusion, or statelessness.

At the tail end of June 2010, the UIDAI website uploaded a "proposed draft bill": the National Identification Authority of India Bill, 2010. Comments were asked to be sent within two weeks, by 13 July 2010. Various individuals and groups have sent in their comments, but have asked that the time to respond be extended so that they may discuss it and understand it more fully before taking their position on the Bill.

One of the provisions that has raised concern is clause 33, which reads:

> 33. Nothing contained in the sub-section (3) of section 30 shall apply in respect of —
>
> (a) any disclosure of information (including identity information or details of authentication) made pursuant to an order of a competent court; or

> (b) any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer not below the rank of Joint Secretary or equivalent in the Central Government after obtaining approval of the Minister in charge.

Although some commentators on the UID project (and that includes me) have written about surveillance, tracking, profiling and social and executive control of the people by the state and its agents, the UIDAI has not acknowledged these concerns so far. This is despite the "Awareness and Communication Report" which the UIDAI commissioned and which advised the authority on how to anticipate and sidestep the unease that people may have, registering that:

> the idea of giving out information and affixing one's thumbprint to a document without fully understanding its implications, compounded with the fact that too many non-state players are visibly involved could pose a barrier to enrolment as well. The fear of individuals being in the government's radar and the ability of various groups to play on this fear is another likely challenge.

Neither the Bill nor any document produced in the process has, however, addressed any of these concerns. What is reflected in the document is only the need to ensure that these anxieties do not come in the way of completing the exercise.

Such a major shift in public policy surely cannot occur without a discussion preceding it, a deliberation on the import, and consequences, of such a change, and a reasoned decision taken on the matter. The constitutionality of such a move is questionable. Among the issues that are likely to arise, there are two that Justice Rajendra Babu raised in the presence of Nandan Nilekani and his team at a consultation held in the National Law School, Bangalore on 23 November 2009: the Constitution guarantees us dignity and privacy, he said. Both seem to have been given a miss in the way the UID project has been conceived.

The combination of UID, NATGRID and the emerging idea of the DNA bank, makes state control of a population a very real possibility. To treat every person as a suspect, and to create systems that would support such a practice, is a highly questionable act of a state. That the State and its agents have faced the charge of being communal, and of having been involved in torture, fake encounters, forced disappearances and complicity in crime adds to the amalgam of concerns. The Bill does not acknowledge it, but those within the system cannot be prosecuted without "sanction" of the powers-that-be. It seems like a prescription for impunity where the protocol for protecting the data is breached from within the state apparatus.

Discussions around the Bill will have to deal with the issues thrown up by the introduction of the element of "national security", especially as it is located within a web of UID, NATGRID and a DNA data bank.

Biometrics

The most disturbing aspect of the UID project is the linking of identity, and rights, entitlements, citizenship and recognition, to biometrics. The UID project has settled on three metrics: facial recognition through the photograph, fingerprints (all eight fingers and two thumbs), and the iris. The UIDAI documents reveal a state of ignorance, and unpreparedness, that is inexplicable. Quotes will set it out most clearly:

In the UIDAI's "Notice Inviting Application for Hiring Biometrics Consultant", for a period of six months starting March 2010, it was written:

> While NIST (the United States agency) documents the fact that the accuracy of biometric matching is extremely dependent on demographics and environmental conditions, there is a lack of a sound study that documents the accuracy achievable on Indian demographics (i.e., larger percentage of rural population) and in Indian environmental conditions (i.e., extremely hot and humid climate and facilities without air-conditioning) ... The 'quality' assessments of fingerprint data is not sufficient to fully understand the achievable de-duplication accuracy. The next step is to acquire biometrics data from the Indian rural conditions in two sessions (with a time difference) and assess the matchability ...

That is, the capacity to capture biometrics with any accuracy *has not even been tested yet*, and the project already has ₹7 crore committed to it for just this year, and the whole apparatus through the NPR moving for it. This demands an explanation.

In a cryptic note, the Notice reads: "The biometric evaluations are statistical. The statistical significance of the results are required to be analysed for the UIDAI."

That is, the margin of error is not yet known.

In "Ensuring Uniqueness: Collecting Iris Biometrics for the Unique *ID* Mission", the report refers to the Biometrics Committee set up under the UIDAI which had, in January 2010, been non-committal about the use of the third biometric, since "... in the absence of empirical Indian data, it is not possible for the committee to precisely predict the improvement in the accuracy of de-duplication to the fusion of fingerprint and iris scores." The document acknowledges "technology risks", including the inability to guarantee biometrics of "high quality across its thousands of enrolment

points". This capture would help in enrolment, but not in authentication since the equipment will not be available in most places. The compromise: "for authentication, the use of fingerprinting will be sufficient". This could spell trouble for calloused hands and marred fingerprints — which would include those doing manual labour and agricultural operations, whose fingerprints cannot be authenticated.

On 17 July 2010, the *Economic Times* reported that "people with 'low-quality' fingerprints and corneal/cataract problems" could "pose difficulties" for the project. "Millions of Indians working in agriculture, construction workers and other manual labourers have worn-out fingers due to a lifetime of hard labour" resulting in "low-quality" fingerprints. The iris scan cannot be done on people with corneal blindness or corneal scars. A study done in 2005 at the All India Institute of Medical Sciences estimated six to eight million people in India had corneal blindness, and many more people would have corneal scars. A Hyderabad based eye institute identified cataract, which results from nutritional deficiency and prolonged exposure to sunlight and ultraviolet rays, and cataract surgery, as almost certain to affect the iris. This is about the people that the UIDAI projects as its main targets. A scientist with the Council of Scientific and Industrial Research is cited as suggesting that "they could use DNA fingerprinting in such cases". Apart from the reduction of a people to a subject-population, these suggestions are inexcusably casual about using techniques that will be of no help to the person so identified.

The draft Bill does not deal with any of these concerns. In clause 3 (1), it declares that "every resident shall be entitled to obtain" a UID number, but nowhere in the Bill is there a clause that no agency may refuse services to a person because they do not have such a number, thus leaving the field open for compulsion. Nowhere in the Bill is there an acknowledgement of the extraordinary powers of surveillance, and invasion of privacy by government and private agencies that the UID will be facilitating, so there are no limits set on the uses of the number and of the networks of information it could be used to generate. So convergence is facilitated, and the person has no control over it, nor is it a wrong in law.

For those who are willing to place their faith in the UID clause 12 May cause them to pause. It reads: "The Authority shall consist of a Chairperson and two part-time members to be appointed by the Central Government", and they may be reappointed, or ejected, by the central government. There are sketchy offences of "intentionally" accessing the UID database and damaging, stealing, altering information or disrupting the data. But it provides no means by which a person whose data is stored to know that such an offence has been committed; and it does not allow prosecution to be launched except on a complaint made by the authority or someone authorised by it. Experience has revealed the failure of regulation; yet it is on regulation by the

authority that a whole population is asked to place its trust. There is no grievance redressal mechanism mandated by law; it may be set up by regulation or it may not. There is a clause in passing that recognises that the data could reach people beyond the borders; but no idea at all on how to deal with that situation.

The demographic information gathered may not be elaborate at the start, but clause 23(b) leaves an opening for expanding the demographic and biometric data that may be collected. Most damning is the passing reference in the general "powers and functions of authority" to the use of the UID number "for delivery of various benefits and services as may be provided by regulation". That is all there is to indicate that service delivery to the poor is the object of this exercise. The issues on which the UID project is piggyback riding for its legitimacy are too serious to be trivialised.

The MoUs the UIDAI has entered into with "registrars" that include banks, state governments and the LIC have been signed with no statutory backing and no legal power to collect, hold and transmit information from and about people. Biometrics has not even been tested, despite Indian demographic and environmental conditions being known to make a significant difference to the quality of biometric capture. In a May 2010 paper prepared for the UIDAI — "A UID Numbering Scheme" — is written: "We expect the UID system to live on for centuries". This, then, is a tagging device that is expected to last well beyond a person's lifetime.

The non-seriousness of the Bill, and the refusal to confront the hard issues, are a slight to democracy which must be remedied before the project progresses to create a *fait accompli*. There are murmurs that the Bill is to be introduced in the monsoon session of Parliament. It would be trite to say that, when biometric accuracy is still in question, and so many questions remain unanswered, it is nowhere near time for parliamentary consideration, or approval.